DETAILED ACTION

This final action is in response to the amendment filed on 01/04/2010. Claims 1-22 are pending and have been considered as follows.

Examiner Note

In light of the applicants' remarks, the examiner hereby withdraws his previous 35 U.S.C. 101 rejections. It is believed that given the context of the applicants' invention as claimed it would be unreasonable to expect one of ordinary skill in the art at the time of the applicants' invention to interpret the applicants' claimed invention as merely a software simulation of an entire network. That is, based on the claim language and context of the applicants' invention, Claims 16-20 are deemed as statutory.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 3, 6, 7, 16 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sit et al (US 6,349,336) in view of Grantges, Jr herein after Grantges (US 6,324,648).

Regarding claim 1, Sit et al teaches

configuring a first control unit, inside a first firewall , the first control unit separate from the first firewall and used to control the network (column 7, lines 15-40: fig. 5, 306);

configuring a proxy server outside the first firewall (Fig. 5, 312); and

Sit et al does not explicitly disclose establishing a session between the first control unit and the proxy server, wherein establishing the session is executed using an access key, nor a step of establishing a connection between the proxy server and a console, to permit remote user management of the network by communication between the first control unit and the console via the proxy server. However, Grantges, discloses a secure gateway, which further discloses

establishing a session between the first control unit and the proxy server, wherein establishing the session is executed using an access key (*column 6, lines 37-67*).

establishing a connection between the proxy server and a console, to permit remote user management of the network by communication between the first control unit and the console via the proxy server (column 14, lines 25-55).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to establish a session using an access key and to permit remote user management of network. The motivation of doing so would have been provide access from a client computer over an insecure public network to one of the plurality destination servers on a secure private network (see Grantges, Column 1, lines 10-15).

Regarding claim 16, Sit et al teaches

a first console residing within an unprotected public network and configured to generate at least one console request message, the console request message including at least one of a request for network management data, a request for Internet Protocol (IP)-Private Branch Exchange (PBX), or a request for status information (column 7, lines 15-40: fig. 5);

a proxy server coupled to the first console, the proxy server configured to pool the at least one request, and to provide access from at least one console to the first control unit and to aggregate and store performance data provided by the first control unit, the proxy server being implemented within a De-Militarized Zone (DMZ) between a protected network and the unprotected public network (fig.2, 255);

a first firewall coupled to the proxy server ((column 7, lines 15-40: fig. 5, 305); and

a first control unit residing within the protected network and coupled to the first firewall, the first control unit configured to receive the at least one request from the proxy server, the first control unit further configured to output at least one response corresponding to the at least one request to the proxy server, the proxy server configured to output the at least one response to the first console (column 7, lines 15-40: fig. 5, 306).

Sit et al does not explicitly disclose that the proxy server being implemented within a De-Militarized Zone. However, Grantges discloses a secure gateway, which further discloses the proxy server being implemented within a De-Militarized Zone (column 4, lines 1-25; Fig. 1).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made such as to being implemented a proxy server within a De-Militarized Zone. The motivation of doing so would have been provide access from a client computer over an insecure public network to one of the plurality destination servers on a secure private network (see Grantges, Column 1, lines 10-15).

Regarding claim 3, Sit et al and Grantges teach the method as in claim 1, and while neither of them expressly disclose, however, Examiner takes Official Notice that configuring the first control unit includes: receiving the proxy server identification information; generating an access key in the first control unit; and sending the access key and first control unit identification information to the proxy server. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to configure a first unit for security purposes as claimed since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 6, Sit et al and Grantges teach the method as in claim 1, and Grantges teaches wherein configuring the proxy server includes: receiving the first control unit identification information(column 6, lines3-13); storing the first control unit identification information in the proxy server(column 6, lines 10-35); adding the first control unit as a first remote device; and exchanging a validation message between the first control unit and the proxy server (column 6, lines 3-30).

Regarding claim 7, Sit et al and Grantges teach the method as in claim 1, while either of them expressly disclose, however, Examiner takes Official Notice that wherein establishing a session between the first control unit and the proxy server includes coupling through a second firewall, the proxy server being inside the second firewall. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to configure a first unit for security purposes as claimed since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 20, Sit et al and Grantges teach the system as in claim 16, and Grantges teaches wherein the proxy server includes processor- executable code, the code performing the steps of: receiving a client request from the first console(Fig.2); writing the at least one request(column 4, fines 1-20, column 5, line 40 to column 6, line 67; reading the at least one request; sending the at least one request to the first control unit (column 4, lines 1-20, column 5, fine 40 to column 6, line 67); sending the at least one request to the first control unit column 4, lines 1- 20, column 5, line 40 to column 6, line 67); receiving the at least one response; and outputting the at least one response to the first console (column 4, lines 1- 20, column 5, line 40 to column 6, line 67)).

3. Claims 9, 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sit et al (US 6,349,336) in view of Grantges, Jr herein after Grantges (US 6,324,648) in further view of Schweitzer (US 2002/0038364).

Regarding claim 9, Sit et al teaches

a first enterprise network (column 7, lines 15-40: fig. 5, 302);

a first control unit coupled to the first enterprise network (column 7, lines 15-40: fig. 5, 306);

a first firewall coupled to the first control unit, the first firewall and first control unit being separate (column 7, lines 15-40: fig. 5, 305);

a public network (column 7, lines 15-40: fig. 5, 301); and a proxy server located outside the first fire wall and implemented within a De-Militarized Zone (DMZ) between the first enterprise network and the public network, the first control unit being configured with proxy server information, the proxy server being configured with first control unit information, the first control unit being further configured to send a first access key to the proxy server, the first control unit and the proxy server configured to establish a communication session based on the first access key, the proxy server to aggregate and store performance data provided by the first control unit.

Sit et al does not explicitly disclose a proxy server located outside the first fire wall and implemented within a De-Militarized Zone (DMZ) between the first enterprise network and the public network, the first control unit being configured with proxy server information, the proxy server being configured with first control unit information, the first control unit being further configured to send a first access key to the proxy server, the first control unit and the proxy server configured to establish a communication session based on the first access key, the proxy server to aggregate and store performance data provided by the first control . However, However, Grantges, discloses a secure gateway a proxy server located outside the first fire wall and implemented within a De-Militarized Zone (DMZ) between the first enterprise network and the public network(column 5, lines 58-68), the first control unit being configured with proxy server information, the proxy server being configured with first control unit information, the first control unit being further configured to send a first access key to the proxy server, the first control unit and the proxy server configured to establish a communication session based on the first access key (*column 6, lines 37-67; column 8, lines40-55*).while neither of them disclose a step of aggregating and storing performance data provided by the first control unit. Schweitzer discloses a system for handling network accounting, which further discloses the proxy server to aggregate and store performance data provided by the first control unit (paragraph [0034]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to establish a session using an access key and to permit remote user management of network. The motivation of doing so would have been provide access from a client computer over an insecure public network to one of the plurality destination servers on a secure private network (see Grantges, Column 1, lines 10-15). The motivation to modify the combined teaching of Sit et al and Grantges such as to sore and aggregate performance would have been to effect improvements in system speed and performance (see Schweitzer paragraph [0007]).

Regarding claim 12, Sit et al teaches

a first enterprise network (column 7, lines 15-40: fig. 5, 302);

a first control unit coupled to the first enterprise network ((column 7, lines 15-40: fig. 5, 306) ;

a first firewall coupled to the first control unit, the first firewall and first control unit being separate (column 7, lines 15-40: fig. 5, 305);

a public network ((column 7, lines 15-40: fig. 5, 301); and

a proxy server, to aggregate and store performance data provided by the first control unit, that includes at least one of a client request handler, a shared request object pool, or a server request handler, the proxy server being implemented within a De-Militarized Zone (DMZ) between the first enterprise network and the public network (column 7, lines 15-40: fig. 5, 305).

Sit et al does not explicitly disclose a proxy server, to aggregate and store performance data provided by the first control unit, that includes at least one of a client request handler, a shared request object pool, or a server request handler, the proxy server being implemented within a De-Militarized Zone (DMZ) between the first enterprise network and the public network (fig.2, 255). However, Grantges, discloses a secure gateway, which further discloses a proxy server, to aggregate and store performance data provided by the first control unit, that includes at least one of a client request handler, a shared request object pool, or a server request handler, the proxy server being implemented within a De-Militarized Zone (DMZ) between the first enterprise network and the public network (column 5, lines58-67), while neither of them disclose a step of aggregating and storing performance data provided by the first control unit. Schweitzer discloses a system for handling network accounting, which further discloses the proxy server to aggregate and store performance data provided by the first control unit *(paragraph [0034]).*

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to establish a session using an access key and to permit remote user management of network. The motivation of doing so would have been provide access from a client computer over an insecure public network to one of the plurality destination servers on a secure private network (see Grantges, Column 1, lines 10-15). The motivation to modify the combined teaching of Sit et al and Grantges such as to sore and aggregate performance would have been to effect improvements in system speed and performance (see Schweitzer paragraph [0007]).

Regarding claim 13, Sit et al and Grantges teach the system as in claim 12, and Grantges teaches wherein the proxy server is configured to receive first control unit identification information, store the first control unit identification information in the proxy server, add the first control unit as a first remote device, and exchange a validation message between the first control unit and the proxy server (column 6, lines 12-35).

4. Claims 2, 4, 5, 8, 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sit et al (US 6,349,336) in view of Grantges, Jr herein after Grantges (US 6,324,648) in further view of Xu et al (US 7,257,837).

Regarding claim 2, Sit et al and Grantges teach the method as in claim 1, while neither of them explicitly configuring a second control unit inside a second firewall, the proxy server being outside the second firewall. However, Xu et al discloses a firewall penetration system for real time media communications, which further discloses that the method further comprising configuring a second control unit inside a second firewall, the proxy server being outside the second firewall (*Fig. 1*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges, Jr. et al such as to include a second firewall. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

Regarding claim 4, ,Sit et al and Grantges teach the method as in claim 3 and while neither of them explicitly disclose wherein receiving the proxy server identification information includes receiving a proxy server host name, a proxy server IP address, and a proxy server port number. Xu et al further discloses wherein receiving the proxy server information includes a proxy server host name, a proxy server IP address, and a proxy server port number (column 2, lines 45-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges, such as to include a proxy server host name, a proxy server IP address, and a proxy server port number. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

Regarding claim 5, Sit et al and Grantges teach the method as in claim 3, while neither of them explicitly discloses wherein receiving the proxy server identification information includes inquiring the proxy server from the first control unit to obtain the proxy server IP address. Xu et al f discloses wherein receiving the proxy server identification information includes inquiring the proxy server from the first control unit to obtain the proxy server IP address (column 4, lines24-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges, Jr. et al such as to include a second firewall. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

Regarding claim 8, Sit et al and Grantges teach the method as in claim 7, while neither of them explicitly discloses connecting between the proxy server and a console, the console being inside the second firewall, the connecting using an IP address facing inside the second firewall. Xu et al further discloses connecting between the proxy server and a console, the console being inside the second firewall, the connecting using an IP address facing inside the second firewall (column 4, lines 24-67; Fig. 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges such as to include a second firewall. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

Regarding claim 17, Sit et al and Grantges teach the system as in claim 16, while neither of them explicitly disclose but does not explicitly discloses a second console coupled to the proxy server, the second console configured to generate at least one other request, the proxy server configured to pool the at least one other request. However, Xu et al discloses a firewall penetration system for real time media communications, which further discloses a second console coupled to the proxy server, the second console configured to generate at least one other request, the proxy server configured to pool the at least one other request(Fig. 1). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges such as to include a second console. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10) teaches a second console coupled to the proxy server, the second console configured to generate at least one other request, the proxy server configured to pool the at least one other request (fig.2, 210).

Regarding claim 18, Sit et al and Grantges teach the system as in claims 16, and Xu et al further disclose that a second firewall coupled to the public network; a second control unit coupled to the second firewall(Fig.1); and

a second enterprise network coupled to the second control firewall, the second control unit being configured with proxy server information, the proxy server being configured with second control unit information, the second control unit being further configured to send a second access key to the proxy server, the second control unit and the proxy server configured to establish a communication session based on the second access key (column 4, line 16 to column 5, line45; Fig.1). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges such as to include and configure a second firewall. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

5. Claims 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sit et al (US 6,349,336) in view of Grantges, Jr herein after Grantges (US 6,324,648) in further view of Devine (US 6,968,571).

Regarding claim 19, Sit et al and Grantges teach the system as in claim 16, while neither of them explicitly discloses wherein the proxy server includes: a client request, a shared request object pool, a server request handler, and a shared request object pool. However Devine et al discloses a secure customer interface for web based data management, which further discloses

A client request handler for receiving a client request from the first console (*column 18, lines 59-67*);

A shared request object pool coupled to the client request handler, the shared request object pool configured to store the at least one request (*column 21, lines 1-15*); and

A server request handler coupled to the shared request object pool*(column 21, lines 13-35)*, the server request handler configured to read the at least one request from the shared request object pool, the server request handler configured to send the at least one request to the first control unit, the server request handler configured to receive the at least one response, the server request handler configured to output the at least one response to the first console(*column 18, line 59 to column 19 , line 20*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges, Jr. et al such as to include in the proxy server includes: a client request, a shared request object pool, a server request handler, and a shared request object pool. One would have been motivated to do so in order to provide a security methodology for connecting users to an enterprise network or extranet over the public Internet as taught by Devine et al (column 1, lines 20-25).

6. Claims 10, 11, 14, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sit et al (US 6,349,336) in view of Grantges, Jr herein after Grantges (US 6,324,648) in further view of Schweitzer (US 2002/0038364) and Xu et al (US 7,257,837).

Regarding claim 10, Sit et al, Grantges and Schweitzer teach the method as in claim 9, and while neither of them explicitly disclose wherein receiving the proxy server identification information includes receiving a proxy server host name, a proxy server IP address, and a proxy server port number. Xu et al further discloses wherein receiving the proxy server information includes a proxy server host name, a proxy server IP address, and a proxy server port number (column 2, lines 45-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Grantges, such as to include a proxy server host name, a proxy server IP address, and a proxy server port number. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10).

Regarding claims 11 and 14, Sit et al , Grantges and Schweitzer teach the system as in claims 9 and 13, and Xu et al further disclose that a second firewall coupled to the public network; a second control unit coupled to the second firewall(Fig.1); and

a second enterprise network coupled to the second control firewall, the second control unit being configured with proxy server information, the proxy server being configured with second control unit information, the second control unit being further configured to send a second access key to the proxy server, the second control unit and the proxy server configured to establish a communication session based on the second access key (column 4, line 16 to column 5, line45; Fig.1). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Sit et al, Grantges and Schweitzer such as to include and configure a second firewall. One would have been motivated to do so in order to establish and maintain real time media communication channels through firewall as taught by Xu et al (column 1, lines 5-10)

Regarding claim 15, Sit et al, Grantges, Schweitzer and Xu et al teach the system as in claim 14, and Xu et al further discloses wherein the proxy server is configured to receive second control unit identification information, store the second control unit identification information in the proxy server, add the second control unit as a second remote device, and exchange a validation message between the second control unit and the proxy server (*column 10 line*

11column 11, line 50). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Sit et al , Grantges and Schweitzer, Jr. et al such as to include second firewall, a second control unit and a second enterprise network. One would have been motivated to do so in order to enable authentication between entities in communication.

7. Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Devine (US 6,968,571) in view of Smith (6,341,311).

Regarding claim 21, Devine teaches

At a proxy server receiving a console request message from a console, the console request message including at least one of a request for network management data, a request for Internet Protocol (IP)-Private Branch Exchange (PBX), or a request for status information (column 8, lines 15-60; column 9, lines 15-35; Fig. 9);

Using a processor, automatically creating a request object; adding the request object to a pool; and notifying a control unit of the request object, the control unit being inside of a firewall (column 14, lines 10-30).

Devine does not explicitly disclose the creation of a request object and addition of the request object to a pool. However, Smith et al discloses a method of detecting data object request, which further disclose the creation of a request object and addition of the request object to a pool (column 21, lines 15-30) .Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made create and addition of request object to a pool of object. The motivation of doing so would have been to utilize deterministic hashing algorithms to allow consistent and predictable identification of a proxy server to be assigned or have residing thereon a particular URL data object (see Smith et al, column 4, lines 25-55)

Regarding claim 22, Devine and Smith et al teach the method as in claim 1, and Devine teaches establishing a data connection with the control unit; receiving a request from the control unit for the request object; sending the request object to the control unit; receiving a response from the control unit based on the request object; and sending the response to the console (column 18, lines59-67; column 21, lines 1-15).

Response to Arguments

8. Applicant's arguments filed 01/04/2010 have been fully considered but they are not persuasive.

- The applicants' remarks with respect to "a first unit, inside a first firewall, the first control unit separate from the first firewall and used to control the network" have been carefully considered but are non-persuasive;
    - The examiner notes that the limitation of "used to control the network" is broad and can include anything that is network related, even the actions performed by the proxy agent as found in the prior art of record;

- The applicants' remarks with respect to "to permit remote user management of the network" have been carefully considered but are non-persuasive;
    - The examiner notes that the functionality of the primary reference would not be altered in such a way in which it would alter the intended critical operation of the prior art of record; Grantges would be merely adding additional functionality to Sit.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Friday from 8:30 AM to 5:00 PM. The examiner can also be contacted via E-mail to schedule a telephone discussion at OSCAR.LOUIE@USPTO.GOV.

If attempts to reach the examiner by telephone or E-mail are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is only available through Private PAIR. If you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 571-272-4100 (local). For more information on the PAIR system or the EBC please visit http://www.uspto.gov/patents/ebc/index.jsp. If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000 (local).

/OSCAR A LOUIE/
04/08/2010

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436